



Privacy and Civil Liberties Impact Assessment  
for the

Project Server

March 19, 2020

**Bureau Reviewing Official**

Timothy H. Skinner  
Bureau Privacy and Civil Liberties Officer  
Office of Privacy, Transparency, and Records  
Department of the Treasury

## Section 1: Introduction

It is the policy of the Department of the Treasury (“Treasury” or “Department”) and its Bureaus to conduct a Privacy and Civil Liberties Impact Assessment (“PCLIA”) when [personally identifiable information](#) (“PII”) is maintained in a system or by a project. PCLIA’s are required for all systems and projects that collect, maintain, or disseminate [PII](#), regardless of the manner in which the information is retrieved.

This assessment is being completed pursuant to Section 208 of the [E-Government Act of 2002](#) (“E-Gov Act”), 44 U.S.C. § 3501, Office of the Management and Budget (“OMB”) Memorandum 03-22, “[OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002](#),” and Treasury Directive 25-07, “[Privacy and Civil Liberties Impact Assessment \(PCLIA\)](#),” which requires Treasury Offices and Bureaus to conduct a PCLIA before:

1. developing or procuring [information technology](#) (“IT”) systems or projects that collect, maintain, or disseminate [PII](#) from or about members of the public, or
2. initiating a new collection of information that: a) will be collected, maintained, or disseminated using [IT](#); and b) includes any [PII](#) permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons. Agencies, instrumentalities, or employees of the federal government are not included.

This PCLIA provides the following information regarding the system or project:

- (1) an overview of its purpose and functions;
- (2) a description of the information collected;
- (3) a description of the how information is maintained, used, and shared;
- (4) an assessment of whether the system or project is in compliance with federal requirements that support information privacy; and
- (5) an overview of the redress/complaint procedures available to individuals who may be affected by the use or sharing of information by the system or project.

This PCLIA is being conducted for the Project Server for the first time.

## Section 2: Definitions

**Agency** – means any entity that falls within the definition of the term “executive agency” as defined in 31 U.S.C. § 102.

**Certifying Official** – The Bureau Privacy and Civil Liberties Officer(s) who certify that all requirements in TD and TD P 25-07 have been completed so a PCLIA can be reviewed and approved by the Treasury Deputy Assistant Secretary for Privacy, Transparency, and Records.

**Collect (including “collection”)** – means the retrieval, receipt, gathering, or acquisition of any PII and its storage or presence in a Treasury system. This term should be given its broadest possible meaning.

**Contractors and service providers** – are private companies that provide goods or services under a contract with the Department of the Treasury or one of its bureaus. This includes, but is not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications.

**Data mining** – means a program involving pattern-based queries, searches, or other analyses of 1 or more electronic databases, where – (a) a department or agency of the federal government, or a non-federal entity acting on behalf of the federal government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals; (b) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and (c) the purpose of the queries, searches, or other analyses is not solely – (i) the detection of fraud, waste, or abuse in a government agency or program; or (ii) the security of a government computer system.

**Disclosure** – When it is clear from its usage that the term “disclosure” refers to records provided to the public in response to a request under the Freedom of Information Act (5 U.S.C. § 552, “FOIA”) or the Privacy Act (5 U.S.C. § 552a), its application should be limited in that manner. Otherwise, the term should be interpreted as synonymous with the terms “sharing” and “dissemination” as defined in this manual.

**Dissemination** – as used in this manual, is synonymous with the terms “sharing” and “disclosure” (unless it is clear from the context that the use of the term “disclosure” refers to a FOIA/Privacy Act disclosure).

**E-Government** – means the use of digital technologies to transform government operations to improve effectiveness, efficiency, and service delivery.

**Federal information system** – means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information owned or under the control of a federal agency, whether automated or manual.

**Final Rule** – After the NPRM comment period closes, the agency reviews and analyzes the comments received (if any). The agency has the option to proceed with the rulemaking as proposed, issue a new or modified proposal, or withdraw the proposal before reaching its final decision. The agency can also revise the supporting analyses contained in the NPRM (e.g., to address a concern raised by a member of the public in response to the NPRM).

**Government information** – means information created, collected, used, maintained, processed, disseminated, or disposed of by or for the federal government.

**Individual** – means a citizen of the United States or an alien lawfully admitted for permanent residence. If a question does not specifically inquire about or an issue does not clearly involve a [Privacy Act system of records](#), the term should be given its common, everyday meaning. In certain contexts, the term individual may also include citizens of other countries who are covered by the terms of an international or other agreement that involves information stored in the system or used by the project.

**Information** – means any representation of knowledge such as facts, data, or opinions in any medium or form, regardless of its physical form or characteristics. This term should be given the broadest possible meaning. This term includes, but is not limit to, information contained in a [Privacy Act system of records](#).

**Information technology (IT)** – means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use: (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product. It includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract. Clinger-Cohen Act of 1996, 40 U.S.C. § 11101(6).

**Major Information system** – embraces “large” and “sensitive” information systems and means “a system or project that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.” OMB Circular A-130, § 6.u. This definition includes all systems that contain [PII](#) and are rated as “MODERATE or HIGH impact” under Federal Information Processing Standard 199.

**National Security systems** – a telecommunications or information system operated by the federal government, the function, operation or use of which involves: (1) intelligence activities, (2) cryptologic activities related to national security, (3) command and control of military forces, (4) equipment that is an integral part of a weapon or weapons systems, or (5) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics, and personnel management. Clinger-Cohen Act of 1996, 40 U.S.C. § 11103.

**Notice of Proposed Rule Making (NPRM)** – the Privacy Act (Section (J) and (k)) allow agencies to use the rulemaking process to exempt particular systems of records from some of the requirements in the Act. This process is often referred to as “notice-and-comment rulemaking.” The agency publishes an NPRM to notify the public that the agency is proposing a rule and

provides an opportunity for the public to comment on the proposal before the agency can issue a final rule.

**Personally Identifiable Information (PII)** –any information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

**Privacy and Civil Liberties Impact Assessment (PCLIA)** – a PCLIA is:

- (1) a *process* conducted to: (a) identify privacy and civil liberties risks in systems, programs, and other activities that maintain [PII](#); (b) ensure that information systems, programs, and other activities comply with legal, regulatory, and policy requirements; (c) analyze the privacy and civil liberties risks identified; (d) identify remedies, protections, and alternative or additional privacy controls necessary to mitigate those risks; and (e) provide notice to the public of privacy and civil liberties protection practices.
- (2) a *document* that catalogues the outcome of that privacy and civil liberties risk assessment process.

**Protected Information** – as the term is used in this PCLIA, has the same definition given to that term in [TD 25-10](#), Section 4.

**Privacy Act Record** – any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual’s education, financial transactions, medical history, and criminal or employment history and that contains the individual’s name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. 5 U.S.C. § 552a (a)(4).

**Reviewing Official** – The Deputy Assistant Secretary for Privacy, Transparency, and Records who reviews and approves all PCLIAs as part of her/his duties as a direct report to the Treasury Senior Agency Official for Privacy.

**Routine Use** – with respect to the disclosure of a record outside of Treasury (i.e., external sharing), the sharing of such record for a purpose which is compatible with the purpose for which it was collected 5 U.S.C. § 552a(a)(7).

**Sharing** – any Treasury initiated distribution of information to government employees or agency contractors or grantees, including intra- or inter-agency transfers or exchanges of Treasury information, regardless of whether it is covered by the Privacy Act. It does not include responses to requests for agency records under FOIA or the Privacy Act. It is synonymous with the term “dissemination” as used in this assessment. It is also synonymous with the term “disclosure” as used in this assessment unless it is clear from the context in which the term is used that it refers to disclosure to the public in response to a request for agency records under FOIA or the Privacy Act.

**System** – as the term used in this manual, includes both federal information systems and information technology.

**System of Records** – a group of any records under the control of Treasury from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. 5 U.S.C. § 552a (a)(5).

**System of Records Notice** – Each agency that maintains a system of records shall publish in the *Federal Register* upon establishment or revision a notice of the existence and character of the system of records, which notice shall include: (A) the name and location of the system; (B) the categories of individuals on whom records are maintained in the system; (C) the categories of records maintained in the system; (D) each routine use of the records contained in the system, including the categories of users and the purpose of such use; (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; (F) the title and business address of the agency official who is responsible for the system of records; (G) the agency procedures whereby an individual can be notified at her/his request if the system of records contains a record pertaining to him; (H) the agency procedures whereby an individual can be notified at her/his request how she/he can gain access to any record pertaining to him contained in the system of records, and how she/he can contest its content; and (I) the categories of sources of records in the system. 5 U.S.C. § 552a (e)(4).

**System Owner** – Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of a system.

## Section 3: System Overview

### Section 3.1: System/Project Description and Purpose

*The US Department of the Treasury (“Treasury” or “The Department”) Office of the Chief Information Officer (OCIO) Project Server focuses on the activities needed to build the Project Portfolio Management (PMP) system procedures and practices. The goal of the Project Server is to enable the OCIO to achieve its mission in providing a comprehensive view of a select portfolio of projects, streamlined communication, proactive risk mitigation, effective decision making, efficient use of resources, and alignment of strategic goals and objectives. In a broader view, Project Server uses enhanced standardization and efficiency to enable Project Managers to improve project management, allows them greater insight and control, and increases discipline and rigor. Project Server also empowers Program Managers to succeed, improve customer satisfaction of Information Technology (IT) projects regarding resources, management of risk, proactive forecasting and prioritization.*

*The table below summarizes its capabilities.*

<b>Capabilities</b>	<b>Example of Business Needs</b>	<b>Potential Solutions</b>
<i>Resources Management</i>	<i>When can we slot new work? How much capacity do we have? How can we justify additional resources? How do we reduce overtime?</i>	<i>Resource forecasts for projects Ability to analyze and review Resource forecasts at multiple levels</i>

<i>Project Information</i>	<i>What is our body of work? Who should we talk to for information? How can we relieve the reporting burden? What is the project status?</i>	<i>Single source of records for project information Ability to categorize and sort projects Ability to generate other reports, such as OCIO pipeline and release plan</i>
<i>Project Schedule</i>	<i>What are the key project dates? What are the official start and end dates? What schedule conflicts are on the horizon? When will our customers get delivery? When will the release occur?</i>	<i>High-level schedules entered for project Auto generated project dashboards Fully loaded integrated master schedule Project dependencies Specialized enterprise calendars</i>
<i>Risk Management</i>	<i>What is our organization's risk load? How can we improve risk communication?</i>	<i>Standardized risk list Single source of records of risks Ability to categorize and communicate key risks to key stakeholders</i>

[PII](#) is used to in the system to assign tasks to users and to monitor Treasury user activity while on the system.

The Treasury OCIO implemented Project Server 2013 as its Project and Portfolio Management (PPM) tool to improve project management processes and activities, specifically scheduling, resource allocation, and risk management.

**Estimated Number of Individuals Whose Personally Identifiable Information is Maintained in the System or by the Project**

<input checked="" type="checkbox"/> 0 – 999	<input type="checkbox"/> 1,000 – 9,999	<input type="checkbox"/> 10,000 – 99,999
<input type="checkbox"/> 100,000 – 499,999	<input type="checkbox"/> 500,000 – 999,999	<input type="checkbox"/> 1,000,000+

**Section 3.2: Authority to Collect**

The authorities for operating this system or performing this project are:

- 5 U.S.C. 301 - Department regulations for the operations of the department, conduct of employees, distribution and performance of its business, the custody, use, and preservation of its records, papers, and property.
- 31 U.S.C. 321 - General authorities of the Secretary establish the mission of the Department of the Treasury.

**Section 4: Information Collection**

**Section 4.1: Relevant and Necessary**

The [Privacy Act](#) requires “each agency that maintains a [system of records](#) [to] maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be fulfilled by statute or by executive order of the President.” 5 U.S.C. § 552a (e)(1). It allows federal agencies to exempt records from certain requirements

(including the relevant and necessary requirement) under certain conditions. 5 U.S.C. § 552a (k). The proposed exemption must be described in a [Notice of Proposed Rulemaking](#) (“NPRM”). In the context of the Privacy Act, the purpose of the NPRM is to give the public notice of a Privacy Act exemption claimed for a system of records and solicit public opinion on the proposed exemption. After addressing any public concerns raised in response to the NPRM, the agency must issue a [Final Rule](#). It is possible for some, but not all, of the [records](#) maintained in the system or by the project to be exempted from the [Privacy Act](#) through the [NPRM/Final Rule](#) process.

**Section 4.1(a)** Please check all of the following that are true:

1.  None of the [PII](#) maintained in the system or by the project is part of a [Privacy Act system of records](#);
  2.  All of the [PII](#) maintained in the system or by the project is part of a [system of records](#) and none of it is exempt from the [Privacy Act](#) relevant and necessary requirement;
  3.  All of the [PII](#) maintained in the system or by the project is part of a [system of records](#) and all of it is exempt from the [Privacy Act](#) relevant and necessary requirement;
  4.  Some, but not all, of the [PII](#) maintained in the system or by the project is part of a [system of records](#) and the records to which the [Privacy Act](#) applies are exempt from the relevant and necessary requirement; and
- Some, but not all, of the [PII](#) maintained in the system or by the project is part of a [system of records](#) and none of the records to which the [Privacy Act](#) applies are exempt from the relevant and necessary requirement.

**Section 4.1(b)**  Yes  No  N/A With respect to [PII](#) maintained in the system or by the project that is subject to the [Privacy Act's](#) relevant and necessary requirement, was an assessment conducted prior to collection (e.g., during [Paperwork Reduction Act](#) analysis) to determine which [PII](#) types (see [Section 4.2](#) below) were relevant and necessary to meet the system's or project's mission requirements? *In addition to login credentials (username and password), Project Server pulls information from the Global Address Book and uses an individual's name and business email address to assign them tasks and indicates when they are available for additional assignments. The minimum number of data elements are used to assign tasks to personnel.*

**Section 4.1(c)**  Yes  No  N/A With respect to [PII](#) currently maintained in the system or by the project that is subject to the [Privacy Act's](#) relevant and necessary requirement, is the [PII](#) limited to only that which is relevant and necessary to meet the system's or project's mission requirements?

**Section 4.1(d)**  Yes  No With respect to [PII](#) maintained in the system or by the project that is subject to the [Privacy Act's](#) relevant and necessary requirement, is there a process to continuously reevaluate and ensure that the [PII](#) remains relevant and necessary?

*The PII maintained in this system is limited to only that which is necessary for identification and authentication of users who require access to the Project Server/Project Online. This includes Treasury personnel to whom tasks are assigned. These users are limited to Treasury employees and contractors.*

*The PII maintained in the system is continuously re-evaluated as part of the continuous monitoring process for Treasury Application and Platform Service –Moderate (APS-M). Annual security assessments are performed, including an annual Privacy Requirements review and necessary updates. Additionally, in accordance with the APS-M System Security Plan, updates to privacy documentation are required after any significant change to the system mission or purpose that results in changes to the type or manner in which PII is collected.*

## **[Section 4.2: PII and/or information types or groupings](#)**

To perform their missions, federal agencies must necessarily collect various types of information. The checked boxes below represent the types of information maintained in the system or by the project. Information identified below is used by the system or project to fulfill the purpose stated in [Section 3.3](#) – Authority to Collect.

Biographical/General Information		
<input checked="" type="checkbox"/> Name	<input type="checkbox"/> Gender	<input checked="" type="checkbox"/> Group/Organization Membership: <u>OCIO</u>
<input type="checkbox"/> Date of Birth	<input type="checkbox"/> Race	<input type="checkbox"/> Military Service Information
<input type="checkbox"/> Home Physical/Postal Mailing Address	<input type="checkbox"/> Ethnicity	<input type="checkbox"/> Personal Home Phone or Fax Number
<input type="checkbox"/> Zip Code	<input type="checkbox"/> Personal Cell Number	<input type="checkbox"/> Alias (including nickname)
<input type="checkbox"/> Business Physical/Postal Mailing Address	<input type="checkbox"/> Business Cell Number	<input type="checkbox"/> Business Phone or Fax Number
<input type="checkbox"/> Personal e-mail address	<input type="checkbox"/> Nationality	<input type="checkbox"/> Mother's Maiden Name
<input checked="" type="checkbox"/> Business e-mail address	<input type="checkbox"/> Country of Birth	<input type="checkbox"/> Spouse Information
<input type="checkbox"/> Personal Financial Information (including loan information)	<input type="checkbox"/> City or County of Birth	<input type="checkbox"/> Children Information
<input type="checkbox"/> Business Financial Information (including loan information)	<input type="checkbox"/> Immigration Status	<input type="checkbox"/> Information about other relatives.
<input type="checkbox"/> Marital Status	<input type="checkbox"/> Citizenship	<input type="checkbox"/> Professional/personal references or other information about an individual's friends, associates or acquaintances.
<input type="checkbox"/> Religion/Religious Preference	<input type="checkbox"/> Device settings or preferences (e.g., security level, sharing options, ringtones).	<input type="checkbox"/> Global Positioning System (GPS)/Location Data
<input type="checkbox"/> Sexual Orientation	<input checked="" type="checkbox"/> User names, avatars, etc.	<input type="checkbox"/> Secure Digital (SD) Card or Other Data stored on a card or other technology
<input type="checkbox"/> Cell tower records (e.g., logs, user location, time etc.)	<input type="checkbox"/> Network communications data	<input type="checkbox"/> Cubical or office number
<input type="checkbox"/> Contact lists and directories (known to contain personal information)	<input type="checkbox"/> Contact lists and directories (not known to contain personal information, but uncertain)	<input type="checkbox"/> Contact lists and directories (known to contain only business information)
<input type="checkbox"/> Education Information	<input type="checkbox"/> Resume or curriculum vitae	<input type="checkbox"/> Other (please describe):
<input type="checkbox"/> Other (please describe):	<input checked="" type="checkbox"/> Other (please describe): <i>Calendar info (e.g. who is out of office/available to accept tasks)</i>	<input type="checkbox"/> Other (please describe): _____

Identifying Numbers	
<input type="checkbox"/> Full Social Security number	<input type="checkbox"/> Health Plan Beneficiary Number
<input type="checkbox"/> Truncated/Partial Social Security number (e.g., last 4 digits)	<input type="checkbox"/> Alien Registration Number
<input type="checkbox"/> Personal Taxpayer Identification Number	<input type="checkbox"/> Business Taxpayer Identification Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)

<input type="checkbox"/> Personal Credit Card Number	<input type="checkbox"/> Business Credit Card Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input type="checkbox"/> Personal Vehicle Identification Number	<input type="checkbox"/> Business Vehicle Identification Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input type="checkbox"/> Personal License Plate Number	<input type="checkbox"/> Business License Plate Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input type="checkbox"/> File/Case ID Number (individual)	<input type="checkbox"/> File/Case ID Number (business) (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input type="checkbox"/> Personal Professional License Number	<input type="checkbox"/> Business Professional License Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input type="checkbox"/> Employee Identification Number	<input type="checkbox"/> Patient ID Number
<input type="checkbox"/> Business Bank Account Number	<input type="checkbox"/> Personal Bank Account Number
<input type="checkbox"/> Commercially obtained internet navigation/purchasing habits of individuals	<input type="checkbox"/> Government obtained internet navigation/purchasing habits of individuals
<input type="checkbox"/> Business License Plate Number (non-sole-proprietor)	<input type="checkbox"/> Driver's License Number
<input type="checkbox"/> Personal device identifiers or serial numbers	<input checked="" type="checkbox"/> Other Identifying Numbers (please describe): <i>Login credentials</i>
<input type="checkbox"/> Passport Number and Passport information (including full name, passport number, DOB, POB, sex, nationality, issuing country photograph and signature) (use "Other" if some but not all elements are collected)	<input type="checkbox"/> Other Identifying Numbers (please describe): _____

Medical/Emergency Information Regarding Individuals		
<input type="checkbox"/> Medical/Health Information	<input type="checkbox"/> Worker's Compensation Act Information	<input type="checkbox"/> Patient ID Number
<input type="checkbox"/> Mental Health Information	<input type="checkbox"/> Disability Information	<input type="checkbox"/> Emergency Contact Information (e.g., a third party to contact in case of emergency)
<input type="checkbox"/> Other (please describe): _____		

Biometrics/Distinguishing Features/Characteristics of Individuals		
<input type="checkbox"/> Physical description/ characteristics (e.g., hair, eye color, weight, height, sex, gender)	<input type="checkbox"/> Signatures	<input type="checkbox"/> Vascular scans
<input type="checkbox"/> Fingerprints	<input type="checkbox"/> Photos	<input type="checkbox"/> Retina/Iris Scans
<input type="checkbox"/> Palm prints	<input type="checkbox"/> Video	<input type="checkbox"/> Dental Profile
<input type="checkbox"/> Voice audio recording	<input type="checkbox"/> Scars, marks, tattoos	<input type="checkbox"/> DNA Sample or Profile
<input type="checkbox"/> Other (please describe): _____	<input type="checkbox"/> Other (please describe): _____	<input type="checkbox"/> Other (please describe): _____

Specific Information/File Types
---------------------------------

<input type="checkbox"/> Taxpayer Information/Tax Return Information	<input type="checkbox"/> Law Enforcement Information	<input type="checkbox"/> Security Clearance/Background Check Information
<input type="checkbox"/> Civil/Criminal History Information/Police Records (government source)	<input type="checkbox"/> Credit History Information (government source)	<input type="checkbox"/> Bank Secrecy Act Information
<input type="checkbox"/> Civil/Criminal History Information/Police Records (commercial source)	<input type="checkbox"/> Credit History Information (commercial source)	<input type="checkbox"/> National Security/Classified Information
<input type="checkbox"/> Protected Information (as defined in Treasury Directive 25-10)	<input type="checkbox"/> Case files	<input type="checkbox"/> Personnel Files
<input checked="" type="checkbox"/> Information provided under a confidentiality agreement	<input type="checkbox"/> Information subject to the terms of an international or other agreement	<input type="checkbox"/> Other (please describe): _____

Audit Log and Security Monitoring Information		
<input checked="" type="checkbox"/> User ID assigned to or generated by a user of Treasury IT	<input checked="" type="checkbox"/> Date and time an individual accesses a facility, system, or other IT	<input checked="" type="checkbox"/> Files accessed by a user of Treasury IT (e.g., web navigation habits)
<input checked="" type="checkbox"/> Passwords generated by or assigned to a user of Treasury IT	<input checked="" type="checkbox"/> Internet or other queries run by a user of Treasury IT	<input type="checkbox"/> Contents of files accessed by a user of Treasury IT
<input type="checkbox"/> Biometric information used to access Treasury facilities or IT	<input type="checkbox"/> Video of individuals derived from security cameras	<input type="checkbox"/> Public Key Information (PKI).
<input type="checkbox"/> Information revealing an individual's presence in a particular location as derived from security token/key fob, employee identification card scanners or other IT or devices	<input type="checkbox"/> Still photos of individuals derived from security cameras.	<input type="checkbox"/> Internet Protocol (IP) Address
<input type="checkbox"/> Other (please describe): _____	<input type="checkbox"/> Other (please describe): _____	<input type="checkbox"/> Other (please describe): _____

Other	
<input type="checkbox"/> Other (please describe: _____)	<input type="checkbox"/> Other (please describe: _____)
<input type="checkbox"/> Other (please describe: _____)	<input type="checkbox"/> Other (please describe: _____)

**Section 4.3: Sources of information and the method and manner of collection**

Treasury Enterprise Directory System (TEDS)	Project Server (internally generated)	End User	Active Directory
<p><b>Specific <u>PII</u> identified in Section 4.2 that was acquired from this source:</b></p> <ul style="list-style-type: none"> <li>• Name</li> <li>• Business e-mail address</li> </ul>	<p><b>Specific <u>PII</u> identified in Section 4.2 that was acquired from this source:</b></p> <ul style="list-style-type: none"> <li>• Group/organization membership: OCIO</li> </ul>	<p><b>Specific <u>PII</u> identified in Section 4.2 that was acquired from this source:</b></p> <ul style="list-style-type: none"> <li>• Project issues and severity</li> <li>• Project tasks</li> </ul>	<p><b>Specific <u>PII</u> identified in Section 4.2 that was acquired from this source:</b></p> <ul style="list-style-type: none"> <li>• Calendar info (e.g. who is out of office)</li> </ul>

• <i>Username</i>		• <i>Project risks</i>	
<b>Manner in which information is acquired from source by the Treasury project/system: (select all that apply):</b>	<b>Manner in which information is acquired from source by the Treasury project/system: (select all that apply):</b>	<b>Manner in which information is acquired from source by the Treasury project/system: (select all that apply):</b>	<b>Manner in which information is acquired from source by the Treasury project/system: (select all that apply):</b>
<input type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group	<input type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group	<input type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group	<input type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group
Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____	Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____	Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____	Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____
<input type="checkbox"/> Received in paper format other than a form.	<input type="checkbox"/> Received in paper format other than a form.	<input type="checkbox"/> Received in paper format other than a form.	<input type="checkbox"/> Received in paper format other than a form.
<input type="checkbox"/> Delivered to the project on disk or other portable device and uploaded to the system.	<input type="checkbox"/> Delivered to the project on disk or other portable device and uploaded to the system.	<input type="checkbox"/> Delivered to the project on disk or other portable device and uploaded to the system.	<input type="checkbox"/> Delivered to the project on disk or other portable device and uploaded to the system.
<input type="checkbox"/> Accessed and downloaded or otherwise acquired via the internet	<input type="checkbox"/> Accessed and downloaded or otherwise acquired via the internet	<input type="checkbox"/> Accessed and downloaded or otherwise acquired via the internet	<input type="checkbox"/> Accessed and downloaded or otherwise acquired via the internet
<input type="checkbox"/> Email	<input type="checkbox"/> Email	<input type="checkbox"/> Email	<input type="checkbox"/> Email
<input type="checkbox"/> Scanned documents uploaded to the system.	<input type="checkbox"/> Scanned documents uploaded to the system.	<input type="checkbox"/> Scanned documents uploaded to the system.	<input type="checkbox"/> Scanned documents uploaded to the system.
<input checked="" type="checkbox"/> Bulk transfer	<input type="checkbox"/> Bulk transfer	<input type="checkbox"/> Bulk transfer	<input type="checkbox"/> Bulk transfer
<input type="checkbox"/> Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).	<input type="checkbox"/> Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).	<input type="checkbox"/> Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).	<input type="checkbox"/> Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).
<input type="checkbox"/> Fax	<input type="checkbox"/> Fax	<input type="checkbox"/> Fax	<input type="checkbox"/> Fax
<input type="checkbox"/> Extracted from notes of a phone interview or face to face contact	<input type="checkbox"/> Extracted from notes of a phone interview or face to face contact	<input type="checkbox"/> Extracted from notes of a phone interview or face to face contact	<input type="checkbox"/> Extracted from notes of a phone interview or face to face contact

<input type="checkbox"/> Other: Please describe: _____	<input checked="" type="checkbox"/> Other: Please describe: <i>Group membership is individually assigned by Project Server Administrator.</i>	<input checked="" type="checkbox"/> Other: Please describe: <i>Employees are provided the option to enter details specific to their projects: status as of date, project narratives (on project details/information and issues).</i>	<input checked="" type="checkbox"/> Other: Please describe: <i>Project Server is able to query Active Directory to be able to pull "free/busy and out of office" information for users that have an account in Project Server</i>
<input type="checkbox"/> Other: Please describe: _____	<input type="checkbox"/> Other: Please describe: _____	<input type="checkbox"/> Other: Please describe: _____	<input type="checkbox"/> Other: Please describe: _____

### **Section 4.4: Privacy and/or civil liberties risks related to collection**

#### Notice of Authority, Principal Uses, Routine Uses, and Effect of not Providing Information

When federal agencies use a form to obtain information from an individual that will be maintained in a [system of records](#), they must inform the individual of the following: “(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (B) the principal purpose or purposes for which the information is intended to be used; (C) the routine uses which may be made of the information as published pursuant to paragraph (4)(D) of this subsection; and (D) the effects on her/him, if any, of not providing all or any part of the requested information.” 5 U.S.C § 522a(e)(3).

**[Section 4.4\(a\)](#)**  Yes  No Is any of the [PII](#) maintained in the system or by the project collected directly from an individual?

**[Section 4.4\(b\)](#)**  Yes  No  N/A Was the information collected from the individual using a form (paper or electronic)?

**[Section 4.4\(c\)](#)**  Yes  No  N/A If the answer to Section 4.4(b) was “yes,” was the individual notified (on the form in which the [PII](#) was collected or on a separate form that can be retained by the individual) about the following at the point where the information was collected (e.g., in a form; on a website).

- The authority (whether granted by statute, or by Executive order of the President) which authorizes the solicitation of the information.
- Whether disclosure of such information is mandatory or voluntary.
- The principal purpose or purposes for which the information is intended to be used.
- The individuals or organizations outside of Treasury with whom the information may be/ will be shared.
- The effects on the individual, if any, if they decide not to provide all or any part of the requested information.

*Users are notified of the above via access agreements and Rules of Behavior, as well as organizational warning banners prior to accessing the Platform.*

#### Use of Social Security Numbers

Social Security numbers (“SSNs”) are commonly used by identity thieves to commit fraudulent acts against individuals. The SSN is one data element that has a heightened ability to harm the individual and requires more protection when used. Therefore, in an effort to reduce risk to individuals and federal agencies, government-wide initiatives aimed at eliminating unnecessary collection, use, and display of SSN have been underway since OMB required agencies to review their SSN practices in 2007.

In addition, the [Privacy Act](#) provides that: “It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual’s refusal to disclose his social security account number.” Pub. L. No. 93–579, § 7. This provision does not apply to: (1) any disclosure which is required by federal statute; or (2) any disclosure of an SSN to any federal, state, or local agency maintaining a [system of records](#) in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual. *Id.* at § 7(a)(2)(A)-(B).

<p><a href="#">Section 4.4(d)</a> <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Does the system or project maintain SSNs?</p> <p><a href="#">Section 4.4(e)</a> <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> N/A Are there any alternatives to the SSNs as a personal identifier? <i>If yes, please provide a narrative below explaining why other alternatives to identify individuals will not be used.</i></p> <p><a href="#">Section 4.4(f)</a> <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> N/A Will an individual be denied any right, benefit, or privilege provided by law if the individual refuses to disclose their SSN? If yes, please check the applicable box:</p> <p><input type="checkbox"/> SSN disclosure is required by Federal statute or Executive Order. ; or</p> <p><input type="checkbox"/> the SSN is disclosed to any Federal, state, or local agency maintaining a <a href="#">system of records</a> in existence and operating before January 1, 1975, and disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual. <i>If checked, please provide the name of the system of records below.</i></p> <p><a href="#">Section 4.4(g)</a> <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> N/A When the SSN is collected, are individuals given notice whether disclosure is mandatory or voluntary, the legal authority such number is solicited, and what uses will be made of it? If yes, please explain below how the notice is provided.</p> <p><i>Social Security Number is not collected or maintained by Project Server. Therefore, no privacy or civil liberties issues were identified</i></p>
--

## First Amendment Activities

The [Privacy Act](#) provides that federal agencies “maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.” 5 U.S.C. § 552a(e)(7).

**Section 4.4(h)**  Yes  No Does the system or project maintain any information describing how an individual exercises their rights guaranteed by the First Amendment?

**Section 4.4(i)** If the system or project maintains information describing how an individual exercises their rights guaranteed by the First Amendment, do any of the following exceptions apply (the information may be maintained if any of the exceptions apply)?

N/A (system or project does not maintain any information describing how an individual exercises their rights guaranteed by the First Amendment so no exceptions are needed)

The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance.

The information maintained is pertinent to and within the scope of an authorized law enforcement activity's

There is a statute that expressly authorizes its collection.

*Project Server does not maintain any information describing how an individual exercises the rights guaranteed by the First Amendment. Therefore, no privacy or civil liberties issues were identified.*

## **Section 5: Maintenance, use, and sharing of the information**

The following sections require a clear description of the system's or project's use of information.

### **Section 5.1: Describe how and why the system or project uses the information it collects and maintains**

Please describe all of the uses of the information types and groupings collected and maintained by the system or project (see [Section 4.2](#)), including a discussion of why the information is used for this purpose and how it relates to the mission of the bureau or office that owns the system.

*The information collected and maintained in the system is used to improve project management processes and activities. Project Server pulls information from the Global Address Book and uses an individual's name and business email address to assign them tasks and indicates when they are available for additional assignments. It can also be used for collaboration.*

*The following types of information are collected: names, business email address, username, group /organization membership, calendar info, project issues and severity, and project tasks. Names and email addresses are used to facilitate communication among Treasury OCIO employees and their managers to provide updates on assigned tasks. When an employee is assigned a task by a manager, the system generates an email only to the Treasury OCIO employee who started the task and also notifies the employee who is to perform the task that it has been assigned to them.*

### **Collecting Information Directly from the Individual When Using it to Make Adverse Determinations About Them**

The [Privacy Act](#) requires that federal agencies "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs." 5 U.S.C. § 552a(e)(2).

**Section 5.1(a)**  Yes  No Is it possible that the information maintained in the system or by the project may be used by Treasury to make an adverse determination about an individual's rights, benefits, and privileges under federal programs (e.g., decisions about whether the individual will receive a financial benefit, get a clearance or access to a Treasury facility, obtain employment with Treasury)?

**Section 5.1(b)**  Yes  No Is it possible that Treasury will share information maintained in the system or by the project with a third party external to the Department that will use the information to make an adverse determination about an individual's rights, benefits, and privileges under federal programs?

**Section 5.1(c)**  Yes  No  N/A If information could potentially be used to make an adverse determination about an individual's rights, benefits, and privileges under federal programs, does the system or project collect information (to the greatest extent practicable) directly from the individual?

*The system collects and maintains name, username and business email. By collecting this information, the user's tasks are reviewed in relation to projects assigned to them. This is to ensure that the user is efficient and focused in completing the tasks assigned to them. It also provides information about the status of tasks assigned to an individual and their performance. This information is useful in project management and tracking progress of the task assigned for more efficient program management. Information maintained in the system regarding employee performance on tasks assigned may be based on input from both the employee and their manager.*

## Data Mining

As required by Section 804 of the [Implementing the 9/11 Commission Recommendations Act of 2007](#) ("9-11 Commission Act"), Treasury reports annually to Congress on its data mining activities. For a comprehensive overview of Treasury's data mining activities, please review the Department's Annual Privacy reports available at: <http://www.treasury.gov/privacy/annual-reports>.

**Section 5.1(d)**  Yes  No Is information maintained in the system or by the project used to conduct "data-mining" activities as that term is defined in the [Implementing the 9-11 Commission Act](#)?

*No privacy and civil liberties risks were identified because the system is not used to conduct data-mining.*

## Section 5.2: Ensuring accuracy, completeness, and timeliness of information collected, maintained, and shared

### Exemption from Accuracy, Relevance, Timeliness, and Completeness Requirements

The [Privacy Act](#) requires that federal agencies "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." 5 U.S.C. § 552a(e)(5). If a particular [system of records](#) meets certain requirements (including the [NPRM](#) process defined in Section 2 above), an agency may exempt the [system of records](#) (or a portion of the records) from this requirement.

**Section 5.2(a)**  Yes  No Is all or any portion of the information maintained in the system or by the project: (a) part of a [system of records](#) and (b) exempt from the accuracy, relevance, timeliness, and completeness requirements in sections (e)(5) of the [Privacy Act](#)?

*Not all of the information maintained in the system is both part of a system of records and exempt from the accuracy, relevance, timeliness, and completeness requirements of the Privacy Act.*

## Computer Matching

The Computer Matching and Privacy Protection Act of 1988 amended the [Privacy Act](#), imposing additional requirements when [Privacy Act systems of records](#) are used in computer matching programs.

Pursuant to the [Privacy Act](#), as amended, there are two distinct types of matching programs. The first type of matching program involves the computerized comparison of two or more automated federal personnel or payroll [systems of records](#) or a system of federal personnel or payroll records with non-federal records. This type of matching program may be conducted for any purpose. The second type of matching program involves the computerized comparison of two or more automated [systems of records](#) or a [system of records](#) with non-federal records. The purpose of this type of matching program must be for the purpose of eligibility determinations or compliance requirements for applicants, recipients, beneficiaries, participants, or providers of services for payments or in-kind assistance under federal benefit programs, or recouping payments or delinquent debts under such federal benefit programs. *See* 5 U.S.C. § 522a(a)(8).

Matching programs must be conducted pursuant to a matching agreement between the source and recipient agencies. The matching agreement describes the purpose and procedures of the matching **and** establishes protections for matching records.

[Section 5.2\(b\)](#)  Yes  No Is any of the information maintained in the system or by the project (a) part of a [system of records](#) and (b) used as part of a matching program?

[Section 5.2\(c\)](#)  Yes  No  N/A Is there a matching agreement in place that contains the information required by Section (o) of the [Privacy Act](#)?

[Section 5.2\(d\)](#)  Yes  No  N/A Are assessments made regarding the accuracy of the records that will be used in the matching program?

[Section 5.2\(e\)](#)  Yes  No  N/A Does the bureau or office that owns the system or project independently verify the information, provide the individual notice and an opportunity to contest the findings, or obtain Data Integrity Board approval in accordance with Section (p) of the [Privacy Act](#) before taking adverse action against the individual?

*None of the records in the system are used as part of a matching program. Project Server is strictly used to manage project, to communicate project information, schedule, resources, risks, issues and status.*

### Ensuring Fairness in Making Adverse Determinations About Individuals

Federal agencies are required to “maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.” 5 U.S.C. § 552a(e)(5). This requirement also applies when merging records from two or more sources where the merged records are used by the agency to make any determination about any individual.

[Section 5.2\(f\)](#)  Yes  No With respect to the information maintained in the system or by the project, are steps taken to ensure all information used to make a determination about an individual is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination?

*In the event that adverse determinations are proposed that include using information from this system, the employee will have an opportunity to refute or provide alternative information explaining the records contained in the system before an adverse determination is made. The employee may also choose to use records in the system to defend against a proposed adverse determination, whether or not the supervisor initially uses information from the system in proposing such a determination.*

## Merging Information About Individuals

**Section 5.2(g)**  Yes  No Is information maintained in the system or by the project merged with electronic or non-electronic information from internal or external sources (e.g., other files or systems)?

**Section 5.2(h)**  Yes  No  N/A Once merged, is the information used in making determinations about individuals (e.g., decisions about whether the individual will receive a financial benefit or payment, get a clearance or access to a Treasury facility, obtain employment with Treasury, etc.)?

**Section 5.2(i)**  Yes  No  N/A Are there documented policies or procedures for how information is merged?

**Section 5.2(j)**  Yes  No  N/A Do the documented policies or procedures address how to proceed when partial matches (where some, but not all of the information being merged matches a particular individual) are discovered after the information is merged?

**Section 5.2(k)**  Yes  No  N/A If information maintained in the system or by the project is used to make a determination about an individual, are steps taken to ensure the accuracy, relevance, timeliness, and completeness of the information as is reasonably necessary to assure fairness to the individual?

*Project Server does not perform large scale, automated, analytical processes that might result in information regarding an individual being merged with information from other files or systems.*

## Policies and Standard Operating Procedures or Technical Solutions Designed to Ensure Information Accuracy, Completeness, and Timeliness

**Section 5.2(l)**  Yes  No  N/A If information maintained in the system or by the project is used to make any determination about an individual (even if it is an exempt [system of records](#)), are there documented policies or standard operating procedures for the system or project that address the accuracy, completeness, and timeliness of the information?

**Section 5.2(m)**  Yes  No Does the system or project use any software or other technical solutions designed to improve the accuracy, completeness, and timeliness of the information used to make an adverse determination about an individual's rights, benefits, and/or privileges (regardless of if it is an exempt [system of records](#))?

*In the event that adverse determinations are proposed that include using information from this system, the employee will have an opportunity to refute or provide alternative information explaining the records contained in the system before an adverse determination is made. The employee may also choose to use records in the system to defend against a proposed adverse determination, whether or not the supervisor initially uses information from the system in proposing such a determination*

## Accuracy, Completeness, and Timeliness of Information Received from the Source

**Section 5.2(n)**  Yes  No Did Treasury or the bureau receive any guarantee, assurance, or other information from any information source(s) regarding the accuracy, timeliness and completeness of the information maintained in the system or by the project?

*OCIO did not receive any information in bulk from an original source that gave assurances regarding accuracy, timeliness, and completeness of the information. All information is derived from other internal Treasury systems.*

## Disseminating Notice of Corrections of or Amendments to PII

**Section 5.2(o)**  Yes  No  N/A Where feasible and appropriate, is there a process in place for disseminating corrections of or amendments to the [PII](#) maintained in the system or by the project to all internal and external information-sharing partners?

**Section 5.2(p)**  Yes  No  N/A Where feasible and appropriate, does the process for disseminating corrections or amendments include notifying the individual whose information is corrected or amended?

*If a user's information is altered and this information is reported by the employee or another source, Project Server administrators will verify and confirm changes with the affected individual and disseminate corrected information to external sharing partners to ensure accuracy.*

## Section 5.3: Information sharing within the Department of the Treasury

### Internal Information Sharing

**Section 5.3(a)**  Yes  No Is [PII](#) maintained in the system or by the project shared with other Treasury bureaus?

**Section 5.3(b)**  Yes  No Does the Treasury bureau or office that receives the [PII](#) limit access to those Treasury officers and employees who have a need for the [PII](#) in the performance of their official duties (i.e., those who have a "need to know")?

*Internal disclosure of the records in Project Server is made only after validating the recipient's need to know the information to perform their official duties.*

### Memorandum of Understanding (MOU)/Other Agreements Limiting Treasury's Internal Use/Disclosure of PII

**Section 5.3(c)**  Yes  No  N/A Is any of the [PII](#) maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement (e.g., agreement with another federal or state agency that provided the information to the Treasury or subject to an international agreement or treaty) that limits or places conditions on Treasury's internal use, maintenance, handling, or disclosure of the [PII](#)?

*There are no MOUs or other agreements limiting Treasury's internal use of the information in the system. Other Treasury Bureaus and Offices will not have access to information contained in the system, except as permitted by the Privacy Act.*

### Internal Information Sharing Chart

Internal Recipient's Name (e.g., bureau or office)	<i>When permitted by the Privacy Act or the System of Records Notice for this system which details a number of Routine Uses to allow disclosure of data from this system.</i>
Purpose of the Sharing	N/A
<a href="#">PII</a> Shared	<i>Information contained in the system</i>
Applicable Statutory or Regulatory or Restrictions on Information Shared	<i>The Privacy Act of 1974 and the OPM/GOVT-2 SORN, <a href="#">Employee Performance File System Records</a>, 71 FR 35347</i>
Applicable Restrictions Imposed by Agreement on Information Shared (e.g., by Treasury agreement)	<i>The Privacy Act of 1974 and the OPM/GOVT-2 SORN, <a href="#">Employee Performance File System Records</a>, 71 FR 35347</i>

with the party that provided the information to Treasury)	
Name and Description of MOU or Other Agreement Restricting Treasury's Internal Use, Maintenance, Handling, or Sharing of <a href="#">PII</a> Received	None
Method of <a href="#">PII</a> Transfer (e.g., paper/oral disclosures/magnetic disk/portable device/email/fax/other (please describe if other)	None

## [Section 5.4: Information sharing with external \(i.e., outside Treasury\) organizations and individuals](#)

### External Information Sharing

[Section 5.4\(a\)](#)  Yes  No Is [PII](#) maintained in the system or by the project shared with agencies, organizations, or individuals external to Treasury?

*External disclosure of the information in Project Server is made only after validating an appropriate routine use published in the OPM/GOVT-2 SORN, [Employee Performance File System Records](#), 71 FR 35347, after identifying a relevant Privacy Act exception, or obtaining the consent of the individual.*

### Accounting of Disclosures

[Section 5.4\(b\)](#)  Yes  No  N/A With respect to [records](#) maintained in the system or by the project that are subject to the [Privacy Act](#), do you maintain a paper or electronic log or other record of the date, nature, and purpose of each disclosure (not including intra-agency disclosures and FOIA disclosures) of a record to any person or to another agency (outside of Treasury) and the name and address of the person or agency to whom the disclosure is made? *See 5 U.S.C § 552a(c).*

[Section 5.4\(c\)](#)  Yes  No  N/A If you do not keep a running tabulation of every disclosure at the time it is made, are you able to reconstruct an accurate and complete accounting of disclosures so as to be able to respond to [Privacy Act](#) requests in a timely fashion?

[Section 5.4\(d\)](#)  Yes  No  N/A With respect to [records](#) maintained in the system or by the project that are subject to the [Privacy Act](#), do you retain the log or other record of the date, nature, and purpose of each disclosure, for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made?

[Section 5.4\(e\)](#)  Yes  No  N/A With respect to [records](#) maintained in the system or by the project that are subject to the [Privacy Act](#), does your bureau or office exempt the [system of records](#) (as allowed by the [Privacy Act](#) in certain circumstances) from the requirement to make the accounting available to the individual named in the record?

[Section 5.4\(f\)](#)  Yes  No  N/A With respect to [records](#) maintained in the system or by the project that are subject to the [Privacy Act](#), does your bureau or office exempt the [system of records](#) (as allowed by the [Privacy Act](#) in certain circumstances) from the requirement to inform any person or other agency about any correction or notation of dispute made by the agency of any [record](#) that has been disclosed to the person or agency if an accounting of the disclosure was made?

*An accounting of external disclosures can be reconstructed from records in the system.*

## Statutory or Regulatory Restrictions on Disclosure

**Section 5.4(g)**  Yes  No In addition to the [Privacy Act](#), are there any other statutory or regulatory restrictions on the sharing of any of the PII maintained in the system or by the project (e.g., 26 U.S.C § 6103 for tax returns and return information)?

*With the exception of the Privacy Act, there are no statutory or regulatory restrictions on external disclosure. External disclosure of the information in Project Server is made only after validating an appropriate routine use published in the OPM/GOVT-2 SORN, [Employee Performance File System Records](#), 71 FR 35347 or after identifying a relevant Privacy Act exception.*

## Memorandum of Understanding Related to External Sharing

**Section 5.4(h)**  Yes  No  N/A Has Treasury (including bureaus and offices) executed a Memorandum of Understanding, or entered into any other type of agreement, with any external agencies, organizations, or individuals with which/whom it shares [PII](#) maintained in the system or by the project?

*There no MOUs or other agreements restricting use or disclosure. External disclosure of the information in Project Server is made only after validating an appropriate routine use published in the OPM/GOVT-2 SORN, [Employee Performance File System Records](#), 71 FR 35347 or after identifying a relevant Privacy Act exception.*

## Memorandum of Understanding Limiting Treasury's Use or Disclosure of PII

**Section 5.4(i)**  Yes  No Is any of the [PII](#) maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement (e.g., agreement with another federal or state agency, an international agreement or treaty, or contract with private vendor that provided the information to Treasury or one of its bureaus) that limits or places conditions on Treasury's internal use or external (i.e., outside Treasury) sharing of the [PII](#)?

*There no MOUs or other agreements restricting use or disclosure. PII in the system can only be shared consistent with the Privacy Act and with the routine uses in the SORN under which Project Server is covered.*

## Memorandum of Understanding Limiting External Party's Use or Disclosure of PII

**Section 5.4(j)**  Yes  No Is any of the [PII](#) maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement in which Treasury limits or places conditions on an external party's use, maintenance, handling, or disclosure of [PII](#) shared by Treasury?

*There no MOUs or other agreements restricting use or disclosure. PII in the system can only be shared consistent with the Privacy Act and with the routine uses in the SORN under which Project Server is covered.*

## External Information Sharing Chart

<b>External Recipient's Name</b>	<i>External disclosure of the information in Project Server is made only after validating an appropriate routine use published in the OPM/GOVT-2 SORN, <a href="#">Employee Performance File System Records</a>, 71 FR 35347 or after identifying a relevant Privacy Act exception.</i>
Purpose of the Sharing PII Shared	<i>As permitted by the Privacy Act and the SORN</i>
Applicable Routine Use/Citation to the <a href="#">SORN</a>	<i>OPM/GOVT-2 SORN, <a href="#">Employee Performance File System Records</a>, 71 FR 35347</i>

Applicable Statutory or Regulatory or Restrictions on Information Shared	<i>The Privacy Act of 1974 and the OPM/GOVT-2 SORN, <a href="#">Employee Performance File System Records</a>, 71 FR 35347</i>
Name and Description of Relevant MOUs or Other Agreements Containing Sharing Restrictions Imposed on Treasury by an External Source or Source/Originating Agency (including description of restrictions imposed on use, maintenance, and disclosure of <a href="#">PII</a> )	None
Method(s) Used to Transfer <a href="#">PII</a> (e.g., paper/ oral disclosures/magnetic disk/portable device/email fax/other (please describe if other))	None

### Obtaining Consent Prior to New Disclosures Not Included in the SORN or Authorized by the Privacy Act

<p><a href="#">Section 5.4(I)</a> <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> N/A Is the individual's consent obtained, where feasible and appropriate, prior to any <b>new</b> disclosures of previously collected records in a <a href="#">system of records</a> (those not expressly authorized by the <a href="#">Privacy Act</a> or contained in the published <a href="#">SORN</a> (e.g., in the routine uses))?</p> <p><i>There are no disclosures of previously collected records in the system of records not expressly authorized by the Privacy Act or contained in the routines uses in the published SORN. If such disclosures become necessary, consent from the individual will be obtained before any disclosure.</i></p>
--

## [Section 6: Compliance with federal information management requirements](#)

Responses to the questions below address the practical, policy, and legal consequences of failing to comply with one or more of the following federal information management requirements (to the extent required) and how those risks were or are being mitigated: (1) the [Privacy Act System of Records Notice Requirement](#); (2) the [Paperwork Reduction Act](#); (3) the [Federal Records Act](#); (4) the [E-Gov Act](#) security requirements; and (5) [Section 508 of the Rehabilitation Act of 1973](#).

### [Section 6.1: Privacy Act System of Records Notice \(SORN\)](#)

For collections of [PII](#) that meet certain requirements, the [Privacy Act](#) requires that the agency publish a [SORN](#) in the *Federal Register*.

**Section 6.1(a)**  Yes  No Does the system or project retrieve [records](#) about an individual using an identifying number, symbol, or other identifying particular assigned to the individual? (see items selected in [Section 4.2](#) above)

**Section 6.1(b)**  Yes  No  N/A Was a [SORN](#) published in the *Federal Register* for this [system of records](#)?

*Treasury .015 - General Information Technology Access Account Records, 80 FR 34963.*

*OPM/GOVT-2, [Employee Performance File System Records](#), 71 FR 35347.*

## **Section 6.2: The Paperwork Reduction Act**

The [PRA](#) requires OMB approval before a federal agency may collect standardized data from 10 or more respondents within a 12 month period. OMB requires agencies to conduct a PIA (a Treasury PCLIA) when initiating, consistent with the [PRA](#), a new electronic collection of PII for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government).

### **Paperwork Reduction Act Compliance**

**Section 6.2(a)**  Yes  No Does the system or project maintain information obtained from individuals and organizations who are not federal personnel or an agency of the federal government (i.e., outside the federal government)?

**Section 6.2(b)**  Yes  No  N/A Does the project or system involve a new collection of [information in identifiable form](#) for 10 or more persons from outside the federal government?

**Section 6.2(c)**  Yes  No  N/A Did the project or system complete an Information Collection Request (“ICR”) and receive OMB approval?

## **Section 6.3: Records Management - NARA/Federal Records Act Requirements**

Records retention schedules determine the maximum amount of time necessary to retain information in order to meet the needs of the project or system. Information is generally either disposed of or sent to the [NARA](#) for permanent retention upon expiration of this period.

### **NARA Records Retention Requirements**

**Section 6.3(a)**  Yes  No Are the records used in the system or by the project covered by NARA’s General Records Schedules (“GRS”) or Treasury/bureau Specific Records Schedule (SRS)?

**Section 6.3(b)**  Yes  No Did NARA approved a retention schedule for the records maintained in the system or by the project?

**Section 6.3(c)**  Yes  No  N/A If NARA did not approve a retention schedule for the records maintained in the system or by the project and the records are not covered by NARA’s GRS or Treasury/bureau SRS, has a draft retention schedule (approved by all applicable Treasury and/or Bureau officials) been developed for the records used in this project or system?

*General records schedule [GRS 3.1, Item 020 \(Information technology operations and maintenance records\)](#) covers reporting on follow-up activities. It indicates a three year retention period after agreement, control measures, procedures, project, activity, or a transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.*

## Section 6.4: E-Government Act/NIST Compliance

The completion of Federal Information Security Management Act (“FISMA”) Security Assessment & Authorization (SA&A) process is required before a federal information system may receive Authority to Operate (“ATO”). Different security requirements apply to National Security Systems.

### Federal Information System Subject to FISMA Security Assessment and Authorization

**Section 6.4(a)**  Yes  No  N/A Is the system a federal [information system](#) subject to FISMA requirements?

**Section 6.4(b)**  Yes  No  N/A Has the system or project undergone a SA&A and received ATO?

*Project Server is a minor application with the boundary of the Treasury Application and Platform Service – Moderate (APS-M). APS-M SA &A package includes Project Server. APS-M package has received ATO on 5/22/2018.*

### Access Controls and Security Requirements

**Section 6.4(c)**  Yes  No Does the system or project include access controls to ensure limited access to information maintained by the system or project?

*In accordance with the APS-M Security Plan and [National Institute of Standards and Technology \(NIST\) 800-53 rev.4](#) requirements, APS-M develops, disseminates, and reviews an organizational Access Control Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance to personnel with system level access to APS-M.*

*User roles and responsibilities are documented in two sections: The roles and responsibilities identified are defined in accordance with the Department of Treasury policy. The policies are disseminated to all users of the APS-M that have associated IT security roles and responsibilities; using a secured common collaboration site, with notifications of new or updated security documentation being facilitated via email.*

*APS-M develops, documents, and disseminates procedures to facilitate the implementation of the access control policy and associated access controls to personnel with system level access to APS-M. Access control policies and procedures are documented within Treasury’s Access Control and Account Management Plan (AC-AMP); which is disseminated to all users of the APS-M who have associated IT security roles and responsibilities via Treasury’s SharePoint site.*

### Security Risks in Manner of Collection

**Section 6.4(d)**  Yes  No In [Section 4.3](#) above, you identified the sources for information used in the system or project and the method and manner of collection. Were any security, privacy, or civil liberties risks identified with respect to the manner in which the information is collected from the source(s)?

*No security, privacy or civil liberties risks were identified with respect to the manner in which the information stored by Project Server is collected from sources.*

### Security Controls When Sharing Internally or Externally

[Section 6.4\(e\)](#)  Yes  No  N/A Are all Treasury/bureau security requirements met in the method of transferring information (e.g., bulk transfer, direct access by recipient, portable disk, paper) from the Treasury project or system to internal or external parties?

*All internal traffic within Project Server is encrypted and adheres to Federal Information Processing Standards (FIPS) 140-2 requirements.*

### Monitoring of Individuals

[Section 6.4\(f\)](#)  Yes  No Will this system or project have the capability to identify, locate, and monitor individuals or groups of people?

*Project Server has the capability to allow managers to identify when an employee is active online and capable of receiving projects. Audit capabilities are performed by Cloud Service Provider (CSP) and adhere to NIST 800-53 rev 4 requirements to ensure proper use of the Project Server. Audit trails and logs are maintained by CSP.*

### Audit Trails

[Section 6.4\(g\)](#)  Yes  No Are audit trails regularly reviewed for appropriate use, handling, and disclosure of [PII](#) maintained in the system or by the project inside or outside of the Department?

*Audit capabilities are performed by the CSP and adhere to NIST 800-53 rev 4 requirements to ensure proper use of the Project Server. Audit trails and logs are maintained by the CSP.*

## [Section 6.5: Section 508 of the Rehabilitation Act of 1973](#)

When federal agencies develop, procure, maintain, or use Electronic and Information Technology (“EIT”), [Section 508 of the Rehabilitation Act of 1973](#) (as amended in 1998) requires that individuals with disabilities (including federal employees) must have access and use (including privacy policies and directives as well as redress opportunities) that is comparable to that which is available to individuals who do not have disabilities.

### Applicability of and Compliance With the Rehabilitation Act

[Section 6.5\(a\)](#)  Yes  No Will the project or system involve the development, procurement, maintenance or use of EIT as that term is defined in [Section 508 of the Rehabilitation Act of 1973](#) (as amended in 1998)?

[Section 6.5\(b\)](#)  Yes  No  N/A Does the system or project comply with all [Section 508](#) requirements, thus ensuring that individuals with disabilities (including federal employees) have access and use (including access to privacy and civil liberties policies) that is comparable to that which is available to individuals who do not have disabilities?

*No privacy or civil liberties risks were identified.*

## [Section 7: Redress](#)

### Access Under the Freedom of Information Act and Privacy Act

[Section 7.0\(a\)](#)  Yes  No Does the agency have a published process in place by which individuals may seek records under the [Freedom of Information Act](#) and [Privacy Act](#)?

*The Treasury FOIA and PA disclosure regulations can be found at 31 C.F.R. Part 1, Subtitle A, Subparts A and C.*

## Privacy Act Access Exemption

[Section 7.0\(b\)](#)  Yes  No Was any of the information that is maintained in [system of records](#) and used in the system or project exempted from the access provisions of the [Privacy Act](#)?

*None of the records in this system of records are exempt from the Privacy Act access requirements.*

## Additional Redress Mechanisms

[Section 7.0\(c\)](#)  Yes  No With respect to information maintained by the project or system (whether or not it is covered by the [Privacy Act](#)), does the bureau or office that owns the project or system have any additional mechanisms other than [Privacy Act](#) and FOIA remedies (e.g., a customer satisfaction unit; a complaint process) by which an individual may request access to and/or amendment of their information and/or contest adverse determinations about denial of their rights, benefits, and privileges under federal programs (e.g., decisions about whether the individual will receive a financial benefit, get a clearance or access to a Treasury facility, obtain employment with Treasury)?

*If audit logs indicate cause for concern of improper use of Project Server, users are allowed to explain their system usage before any adverse action is taken, as per Treasury policy.*

## Approval Signature

---

Timothy H. Skinner  
Bureau Privacy and Civil Liberties Officer  
Office of Privacy, Transparency, and Records  
U.S. Department of the Treasury